InfoCage モバイル防御

インストールガイド

InfoCage モバイル防御
Version 3.6
インストールガイド
(Windows XP/2000 用)

目 次

第1章　はじめに

このたびは、InfoCage モバイル防御 をお買い上げいただき、まことにありがとうございます。
InfoCage モバイル防御は、パソコンからの情報漏洩を防止するため、認証を受けていない人がそのパソコンを使うことを防止したり、データを暗号化して読めないようにしたりすることができる情報漏洩対策セキュリティソフトウェアです。

InfoCage モバイル防御には、メディア鍵で認証する「メディア鍵認証方式」と、パスワードで認証する「パスワード認証方式」があります。

* 「メディア鍵認証方式」と「パスワード認証方式」の併用はできません。
インストール時に選択してください。
パスワード認証方式を選択した場合、ログオン認証にパスワードまたは FeliCa カードのどちらかを選択できます。

InfoCage モバイル防御で情報漏洩を防止するためには、インストール時にパソコンを使用する人を認証する「鍵」の作成または「パスワード」の設定を行い、その後保護が必要なファイルの暗号化を行う必要があります。
本インストールガイドに従ってそれぞれ設定を行ってください。
インストール後はパソコンを再起動する必要があります。他のプログラムを実行中の場合は、終了させてください。

1.1 InfoCage モバイル防御の特徴

メディア鍵認証方式

■パソコンのロック

鍵を格納したリムーバブルメディア等をパソコンから抜くことでパソコンをロックし、操作ができないようにすることができます。また、鍵を装着することでロックを解除できます。

※ パソコンのロック機能のみでは情報漏洩対策は万全ではありません。
重要なファイルは必ず暗号化してください。

■ファイルの暗号化

ドライブ、フォルダ単位でデータの暗号化を行い、鍵となるリムーバブルメディアが装着された場合のみファイルアクセスが可能になります。
パソコン内のデータだけでなく、リムーバブルメディア内のデータも暗号化できます。

■データの抜き取り防止

認証されていないリムーバブルメディアへのコピーを禁止して、情報の抜き取りを防止します。

※管理者の設定により、「外部メディア自動暗号機能」も併用可能です。

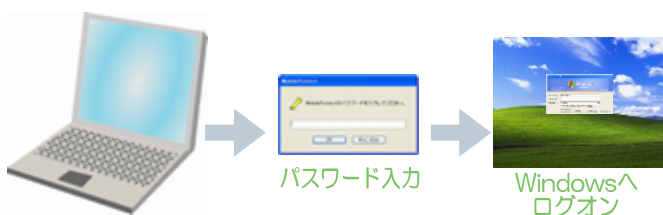
● 「鍵」とは

例えば鍵がなければドアが開かないのと同様に、リムーバブルメディアの「鍵」がなければパソコンの情報にアクセスできないようにするものです。

● 「鍵情報」とは

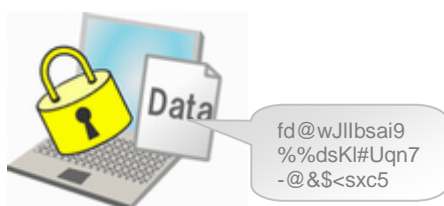
各メディアに作成した「鍵」のバックアップデータを「鍵情報」といい、「鍵」となるメディアとは別のリムーバブルメディアなどに保存しておきます。
「鍵」を保存したリムーバブルメディア内のデータを紛失した場合は、「鍵情報」を元に復旧します。

パスワード認証方式

■パソコンのロック

InfoCage モバイル防御のパスワードが正しく入力された場合のみ、Windows にログオン可能になります。

■FeliCa カードでの認証

Windows へのログオンを FeliCa カードで認証することもできます。

■ファイルの暗号化

ドライブ、フォルダ単位で暗号化を行います。
パスワードを正しく入力し、Windows にログオンすると暗号化ファイルは自動で復号され、ファイルアクセスが可能になります。

■外部メディア自動暗号機能

所属するグループ内でのみ使用が許可されるリムーバブルメディアを設定することができ、この許可されたリムーバブルメディア（許可外部メディア）へはデータは自動的に暗号化されて書き込まれ、読み込むときには自動的に復号されます。

※ InfoCage モバイル防御の管理者が本機能の設定をしている場合に使用可能です。

- セキュリティチップ（TPM）でのセキュリティ強化

セキュリティチップ（TPM）搭載のパソコンをお使いの場合、セキュリティチップ（TPM）が有効となっている場合により強固なセキュリティを実現します。

* InfoCage モバイル防御の管理者がセキュリティチップ（TPM）を有効にする設定をしている場合に使用可能です。

1.2　スタンドアローンモードとネットワークモード

InfoCage モバイル防御では、パソコン単体で運用するスタンドアローンモードと、
InfoCage モバイル防御 管理サーバがクライアントの設定などを管理するネットワークモードがあります。
インストール時に運用方法を選択する必要がありますので、InfoCage モバイル防御の管理者に確認後、インストールを実施してください。

- スタンドアローンモード

それぞれのパソコンを単体で運用します。

- ネットワークモード

スタンドアローンモードの機能に加え、サーバと連携する運用モードです。
InfoCage モバイル防御の管理者がユーザ登録やポリシー設定を行い、管理サーバがクライアントの管理・監視・警告を行います。

第2章　インストールの前にお読みください

2.1　　インストールの流れ

1. セットアッププログラムのカスタマイズ（管理者が設定する場合）

2. リムーバブルメディアを用意

鍵や鍵情報を保存するリムーバブルメディアを用意（メディア鍵認証方式のみ）

3. インストール

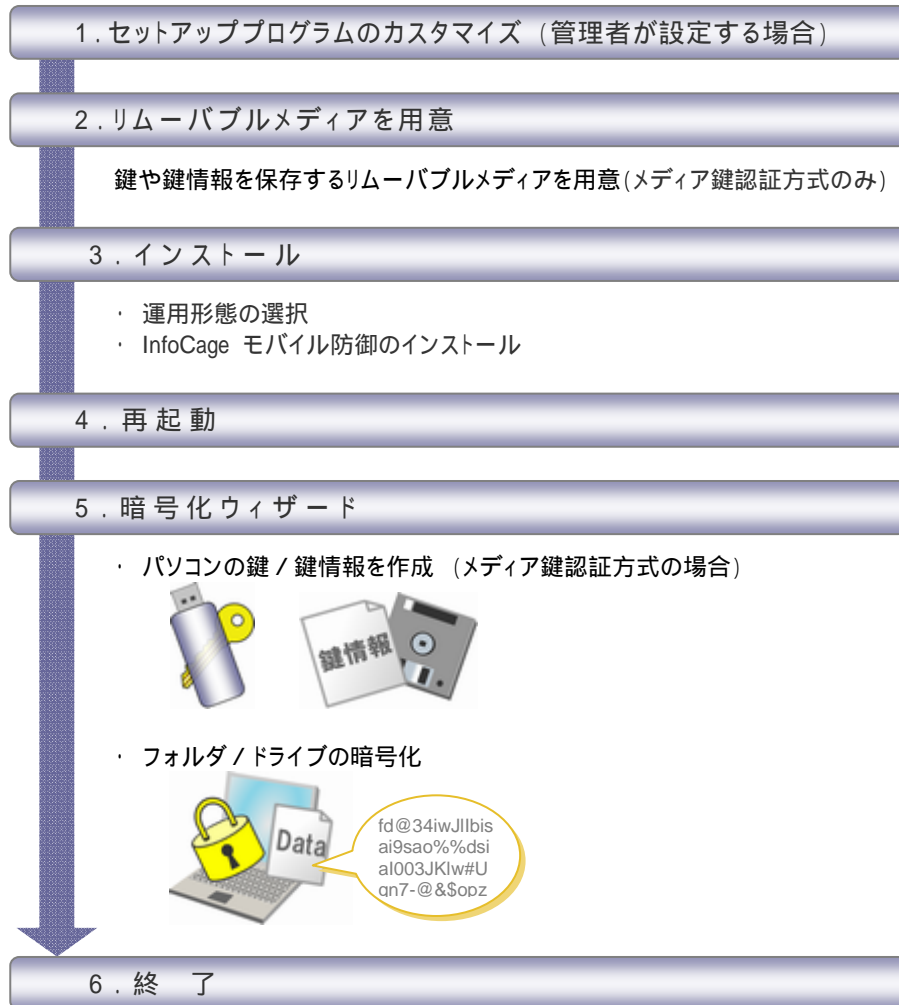
- 運用形態の選択
- InfoCage モバイル防御のインストール

4. 再起動

5. 暗号化ウィザード

- パソコンの鍵／鍵情報を作成（メディア鍵認証方式の場合）

- フォルダ／ドライブの暗号化

6. 終　了

運用形態等が管理者によってあらかじめ設定されている場合は、本ガイドの操作手順と異なる場合があります。

2.2 注意事項

1. お願い

   ・ インストールおよびアップグレードインストールを行う前に、「2.3 【導入前の注意事項】確認チェックシート」を使用して、インストール環境の確認を行ってください。

   ・ 万が一に備え、大切なデータはバックアップを取ってから使用してください。

2. 動作環境

   ・ オペレーティングシステム
   Windows XP Professional （日本語版）
   Windows XP Home Edition （日本語版）
   Windows XP Tablet PC Edition （日本語版）
   Windows XP Tablet PC Edition 2005 （日本語版）
   Windows 2000 Professional （日本語版）

   * Microsoft 社から提供される最新パッチや ServicePack の適用をお奨めします。

   * ネットワークモードで運用する場合は、Windows XP は ServicePack 1 または 2、Windows2000 は ServicePack 4 の適用が必要です。

   ・ メモリ
   128MB 以上

   ・ ハードディスクの空き容量
   本製品のインストールドライブには 25MB 以上の空き容量が必要です。インストールの際にはセットアップ情報を展開するために、さらに 20MB 以上の空き容量が必要です。また、暗号化する際には、以下の空き容量が必要です。
   必要な空き容量 ＝ 暗号化対象ファイルの中で最大のファイルと同等の容量 ＋（ドライブ容量×0.02）
   （上記は最低限必要な容量です。暗号化処理は十分な空き容量がある状態で行ってください。）
   初めて暗号化処理を行う場合は全てのドライブのごみ箱を暗号化するため、暗号化指定していないドライブにも上記の空き容量が必要となりますのでご注意ください。

3. インストール前の注意事項

   ・ InfoCage モバイル防御と共存できないアプリケーションと併用すると、正しく動作しない場合があります。インストール前に「2.2 注意事項 10. アプリケーション競合問題について」を必ず確認してください。

   ・ インストールは、コンピュータの管理者権限を持つユーザで、日本語または英語以外の文字を含まないユーザ名で行ってください。
   InfoCage モバイル防御 ユーティリティの操作もコンピュータの管理者で行ってください。
   また、Windows XP の「別のユーザとして実行」機能は使用しないでください。

   ・ プロダクト ID はライセンス証書に記載されています。

   ・ NTFS ファイルシステムの暗号化、または圧縮されたファイルは InfoCage モバイル防御では暗号化できないため、NTFS ファイルシステムの暗号化、または圧縮している場合は、InfoCage モバイル防御をインストールする前に解除してください。

   ・ 仮想ドライブの割り当ては行わないでください。
   （SUBST コマンドおよび MOUNTVOL コマンドを使用、または「コンピュータの管理」－「ディスクの管理」でドライブ文字またはパスの変更より「次の空の NTFS フォルダにマウントする」を使用など）

   ・ InfoCage モバイル防御をインストール後は、コントロールパネル等からユーザのログオンやログオフの方法を変更することができなくなります。セキュリティ強化のため、「Ctrl+Alt+Del」キーを押下する画面を表示するように設定を変更する場合は、インストール前に設定変更してください。

4. インストール後の注意事項

- インストール時に入力するスーパーバイザパスワード／ユーザパスワードは、InfoCage モバイル防御 ユーティリティの起動時、鍵の復旧時、アンインストール時に必要になりますので、絶対に忘れないように注意してください。
- InfoCage モバイル防御を正常にインストールした後に、同じバージョンの setup.exe を実行しないでください。
- InfoCage モバイル防御の管理者の設定によっては、InfoCage モバイル防御をインストール後、Windows のセーフモードでの起動ができなくなる場合があります。
- Windows XP に InfoCage モバイル防御をインストールすると、OS 標準のバックアップ機能が使用できなくなります。バックアップを行う場合は、InfoCage モバイル防御のインストールフォルダ（通常は ¥Program Files¥NEC¥InfoCageCE）内の ¥tools¥MPBackup.exe を使用してバックアップを行ってください。操作方法については、「InfoCage/モバイル防御 ユーザーズガイド」の 「バックアップツールの利用」の項を参照してください。
- Windows XP に InfoCage モバイル防御をインストールすると、ユーザ選択画面が表示されなくなり、「簡易ユーザ切り替え」ができなくなります。また、シャットダウン時の画面が「コンピュータの電源を切る」（ボタン選択）画面から、「Windows のシャットダウン」（プルダウンメニュー選択）画面に変更されます。
- InfoCage モバイル防御をインストールすると、OS 標準の「システムの復元」が使用できなくなります。
- InfoCage モバイル防御をインストールすると「Windows へようこそ」画面が通常のログオン画面に変更されます。

  * Windows の設定によっては、「Windows へようこそ」画面は表示されません。
- InfoCage モバイル防御インストール後は ファイルシステムの変更（FAT および FAT32 から NTFS へのコンバート）は行えません。コンバートを行う場合は、一旦 InfoCage モバイル防御をアンインストールしてから行ってください。
- InfoCage モバイル防御インストール後は、OS の再インストールおよびリカバリ、または内蔵ハードディスクのフォーマットは行わないでください。これらを行う場合は、一旦 InfoCage モバイル防御をアンインストールしてから行ってください。

5. 暗号化について

- 暗号化を実行する前に、常駐プログラムを含むすべてのアプリケーションを必ず終了させてください。アプリケーションが使用しているファイルは、暗号化できない場合があります。
- 暗号化や暗号化解除（復号）を行う場合、暗号化／復号処理の途中で、強制終了、Windows のロック、スクリーンセーバの設定の変更を行うとファイルが不正になりますので、絶対に行わないでください。
- 以下の操作を行うとデータを正しく参照できなくなりますので、絶対に行わないでください。OS にログオンできなくなった場合などでデータを退避させたい場合でも、何も操作を行わず速やかに InfoCage モバイル防御製品保守担当までご相談ください。

  * 暗号化したハードディスクを別のパソコンに接続し、データを移動する
  * セーフモードで起動し、暗号化したハードディスクから別のドライブにデータを移動する
- NTFS ファイルシステムの場合、暗号化するファイルとフォルダは、SYSTEM アカウントの変更権限が必要です。

＜変更方法＞
（Windows XP Professional および Windows 2000 Professional のみ変更可能です。）
1 SYSTEM アカウントを変更したいフォルダを右クリックし、表示されるメニューの中から「プロパティ」をクリックしてください。
2 「セキュリティ」タブを選択してください。
3 「グループ名またはユーザ名」から「SYSTEM」を選択し、「アクセス許可」の「フルコントロール」の「許可」にチェックを入れ、「OK」をクリックしてください。

- NTFS ファイルシステムの暗号化または圧縮されたファイルは暗号化できません。
- 暗号化指定したフォルダを共有設定しないでください。
- 旧バージョンの InfoCage モバイル防御で暗号化したリムーバブルメディアおよびハードディスクドライブを本バージョンの InfoCage モバイル防御がインストールされているパソコンに装着した場合、一部のファイルが正常に読み込みできないことがあります。

・ 万が一、使用中に次のような現象が発生した場合は、大切なデータを損失する可能性がありますので、現象が発生した状態のまま何も操作を行わず、速やかに InfoCage モバイル防御製品保守担当までご相談ください。

  * 暗号化したはずのファイルが読み書きできない（文字化けなど）
  * OS にログオンできない
  * 作成した鍵が使用できない（メディア鍵認証方式の場合）

6. アップグレードインストールの注意事項

・ アップグレードインストールを行う場合、既にインストール済みの InfoCage モバイル防御をアンインストールする必要はありません。

・ 暗号化した外付けハードディスクドライブおよびリムーバブルディスクがある場合は、必ずパソコンに装着した状態でアップグレードインストールを行ってください。パソコンから取り外した状態でアップグレードした場合、一部のファイルが正常に読み込みできないことがあります。

・ お使いのバージョンによってはアップグレードインストールの途中で数回再起動を行う場合があります。メッセージにしたがって操作してください。

・ 外部メディア自動暗号機能や FeliCa カードでの認証機能については、セットアッププログラムのカスタマイズを行い、アップグレードインストールすることで、各機能が有効になります。カスタマイズ方法については、「InfoCage モバイル防御 管理者ガイド」を参照してください。

・ バージョンにかかわらずアップグレードインストール後も設定を引き継ぐものは以下の通りです。

  * スーパーバイザパスワード／ユーザパスワード
  * 鍵および鍵情報（InfoCage モバイル防御 Ver1.0 で鍵情報をネットワーク共有フォルダに作成している場合もそのまま引き継がれます。）
  * 暗号化指定されたドライブ／フォルダ
  * 管理サーバでの設定内容（ネットワークモードで運用している場合）
  * インストール先のフォルダ
  * クライアント初期設定ツールでセットアッププログラムをカスタマイズしてインストールした設定内容
  * その他のユーティリティでの設定内容
    （InfoCage モバイル防御ユーティリティおよびメディア暗号ユーティリティ）

・ Ver3.5 より以前のバージョンからアップグレードインストールを行った場合に変わるものは以下の通りです。

  * プログラム名
    [MobileProtect]
    ↓
    [InfoCage／モバイル防御]

  * スタートメニューからの起動方法
    [すべてのプログラム] －[MobileProtect]
    ↓
    [すべてのプログラム] － [NEC] － [InfoCage／モバイル防御]

  * ユーザーズガイド
    [MobileProtect オンラインマニュアル]
    ↓
    [InfoCage／モバイル防御 ユーザーズガイド]

7. メディア鍵認証方式の注意事項

(1) 事前にご準備いただくもの

インストールにはリムーバブルメディアが2個必要です。

ご使用にあたっては、鍵を格納するリムーバブルメディア(*1)と、鍵情報を格納するためのリムーバブルメディア(*2)が必要です。各リムーバブルメディアはインストール前に再度フォーマットしておいてください。

* リムーバブルメディアをフォーマットせずに使用した場合、鍵の作成や復旧ができない場合があります。

*1:USBメモリ、フラッシュメモリカード、モバイルディスクの他、サーバの共有フォルダが使用できます。
(推奨:USBメモリ)
*2:フロッピーディスク、USBメモリ、フラッシュメモリカード、モバイルディスクが使用できます。
ただし、別売の「InfoCage モバイル防御管理サーバ」と連携して動作するネットワークモードで使用する場合は、鍵情報はサーバに保存されますので、鍵情報を格納するメディアは必要ありません。

(2) 注意事項

- 鍵情報の保存
  スタンドアローン運用時、鍵情報は鍵を作成したメディアには保存できません。

- 鍵について
  InfoCage モバイル防御で保護されたパソコンを使用する際には、必ず鍵を作成したメディアを装着した状態で使用してください。
  鍵を装着しない状態で使用した場合は、データが不正になる場合があります。
  また、鍵を装着していない場合、ごみ箱へのファイル削除が拒否されます。

- 鍵情報について
  「鍵情報」を紛失すると「鍵」の復旧ができませんので、「鍵情報」を保存したリムーバブルメディア内のデータを絶対に紛失しないように注意してください。

8. パスワード認証方式の注意事項

セキュリティチップ(TPM)を使用している場合、以下の操作を行うと、暗号化されたファイルにアクセスできなくなりますので絶対に行わないでください。これらを行う場合は、一旦 InfoCage モバイル防御をアンインストールしてから行ってください。

* BIOS でセキュリティチップを「使用しない」に設定を変更する
* BIOS のアップデートなどで設定値を初期化する
* セキュリティチップユーティリティをアンインストールする

9. InfoCage 持ち出し制御 クライアントと併用する場合

InfoCage 持ち出し制御 クライアントがインストールされているパソコンに InfoCage モバイル防御をインストールする場合は、以下の手順を実施してください。

(1) InfoCage 持ち出し制御をアンインストールする。

(2) InfoCage モバイル防御をインストールし、再起動後に暗号化を行う。

(3) InfoCage 持ち出し制御 クライアントをインストールする。

10. アプリケーション競合問題について

次のアプリケーションソフトは、InfoCage モバイル防御と同時に利用、または InfoCage モバイル防御がインストールされた環境で利用すると、問題が発生することがあります。
これらのアプリケーションソフトは InfoCage モバイル防御をインストールする前にアンインストールしておいてください。アンインストールできない場合は使用しないでください。

* 下記はこれまで報告のあったアプリケーションの一覧を記載しております。記載のないアプリケーションの動作を保証するものではありません。

InfoCage モバイル防御と共存できないアプリケーション

アプリケーションの種類
・他のファイル暗号化ソフト、独自のログオン認証を行うソフト
・仮想マシン環境構築ソフト(VMware、Microsoft VirtualPC など)
・データバックアップ、リカバリソフト (StandbyDisk、StandbyDisk Solo、StandbyDisk Solo RB、FINALDATA、Acronis True Image LE、Acronis True Image 8.0 など)
・一部のディスクイメージ(HDD バックアップ)作成ソフト(V2i Protector など)
・ティアック株式会社 Swipe FINGERPRINT USB メモリ および NEC 製ノートパソコン内蔵の指紋センサ以外を使用する指紋認証システム (NEC 製ノートパソコン内蔵の指紋センサを使用した認証システムと、InfoCage モバイル防御の認証システムとの併用が可能です。ただし、Swipe FINGERPRINT USB メモリのように連携させることはできません。)
・一部のライティングソフト(B's CLiP など)
・一部の PC プレインストールソフト(IBM/レノボ製 PC に付属のバックアップソフト「Rapid Restore Ultra/Rescue and Recovery」、松下電器製 PC に搭載されている「オプティカルディスク省電力ユーティリティ」 など)
・一部のウイルス対策ソフト(GRISOFT AVG Anti-Virus、eTrust Antivirus など)
・Norton SystemWorks(Norton Utilities)の Norton Protection(ごみ箱機能) 使用している場合は InfoCage モバイル防御をインストールする前に解除してください。 ＜解除方法＞ 1.デスクトップの「Norton ごみ箱」のアイコンを右クリックし、「プロパティ」をクリックしてください。 2.「Norton Protection」タブを選択してください。 3.プルダウンメニュー「ドライブ」で、ドライブを選択し、「保護を有効にする」チェックを外してください。 ※必ず全ドライブ無効にしてください。 4.「OK」をクリックしてください。 ※ 設定を変更しない場合、ファイルの暗号化や復号に失敗する可能性があります。

使用に制限のあるアプリケーション

アプリケーションの種類	対策
CD-R 等ライティングソフト	
・Windows XP 標準の CD 書き込み機能	ファイルを書き込みする場合は、暗号化されていないフォルダにファイルをコピーもしくは移動した後に操作を行うことで利用可能
・DirectCD	
ウイルス対策ソフト	
・SymantecAntiVirusCorprateEdition10.0 (MR2 MP2 より以前のバージョン)	パッチ適用により利用可能
・Symantec Client Security 3.0.2 (MR2 MP2 より以前のバージョン)	
・Norton AntiVirus2006	
その他ソフト	
・Symantec pcAnywhere	・pcAnywhere→モバイル防御の順でインストールすることで利用可能 ・モバイル防御→pcAnywhere の順でインストールする際は、パッチ適用で利用可能
・NETWIZARD	・「ReachOut サービスを停止しました」エラーを閉じてログオンすることで利用可能。 ・閉じずにログオンした場合は Ctrl+Alt+Del を押下してエラーを再表示し閉じることにより利用可能。
・BIGLOBE リモートアクセスサービス VPN クライアント	・VPN ソフト→モバイル防御の順番でインストールすることで利用可能
・ローミングクライアント	以下のどちらかで利用可能 ・ローミングクライアント→モバイル防御の順でインストール。 ・ローミングクライアントのレジストリを編集。 ただし、ドメイン環境使用時には上記回避策のみではドメインログオンができなくなります。モバイル防御の初期設定ファイルを置換することで利用可能。
・WebSAM WinShare	・WebSAM WinShare→モバイル防御の順でインストールすることで利用可能。
・Pointsec	・ディスク暗号による暗号化環境での利用不可。

* 下記のライティングソフトは InfoCage モバイル防御とは併用が可能であることを確認しています。
  - RecordNow
  - B'sRecorder Gold
  - Easy CD Creator

2.3　【導入前の注意事項】確認チェックシート

氏名＿＿＿＿＿＿＿＿

	確 認 事 項	チェック欄	
		メディア鍵 認証方式	パスワード 認証方式
1	重要なデータは、念のためバックアップを取ること。		
2	鍵用のメディア、あるいはサーバを用意すること。		
3	十分な空き容量が各ドライブにあること。 ※暗号化を実行する際、テンポラリ（一時作業スペース）として以下の空き容量がドライブ毎に必要になります。 必要な空き容量 ＝ 暗号化対象ファイルの中で最大のファイルと同等の容量 ＋ （ドライブ容量×0.02） （上記は最低限必要な容量です。暗号化処理は、十分な空き容量がある状態で行ってください。） ※ただし、初めて暗号化処理を行う場合は全てのドライブのごみ箱を暗号化するため、暗号化指定していないドライブにも上記の空き容量が必要となりますのでご注意ください。		
4	フォルダ名やファイル名に日本語、または英語以外の文字列を使用している場合は、日本語、または英語に変更すること。		
5	共存不可のアプリケーションの確認・対策を行うこと。 ※「2.2 注意事項 10 アプリケーション競合問題について」を参照		
6	暗号化するフォルダやファイルに SYSTEM アカウントの変更権限があることを確認すること。		
7	デュアルブートマシンでないこと。		
8	仮想ドライブを割り当てていないこと。		

※このシートをコピーして使用してください。

第3章　インストール

* アップグレードインストールを行う場合は、「第 5 章アップグレードインストール」を参照してください。

3.1　Step1

注意

インストールを行う前に、InfoCage モバイル防御を使用するパソコンの環境をチェックしてください。
(環境のチェック方法)
InfoCage モバイル防御が格納されているメディア (例 CD-ROM) 内の¥2K_XP¥Tools¥環境チェックUTL¥MPEnvChk.EXEを実行してください。

* CD-ROM からコピーして使用する場合は、環境チェック UTL フォルダをデスクトップなどにコピーしてから実行してください。(MPEnvChk.EXE は実行ファイルのみをコピーしても動作しません。)

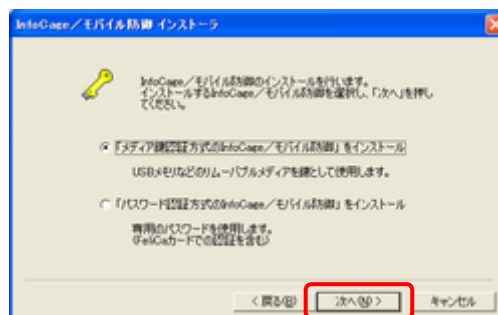
問題が見つかった場合は、すべて対処してください。画面内の「対処方法」をクリックすると、対処方法が表示されます。

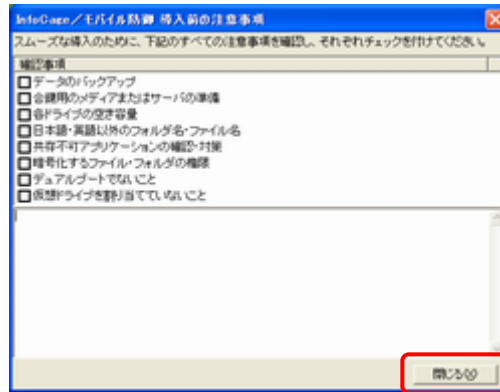
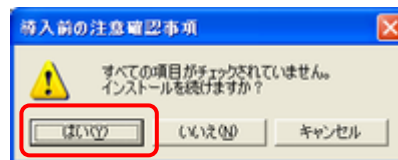
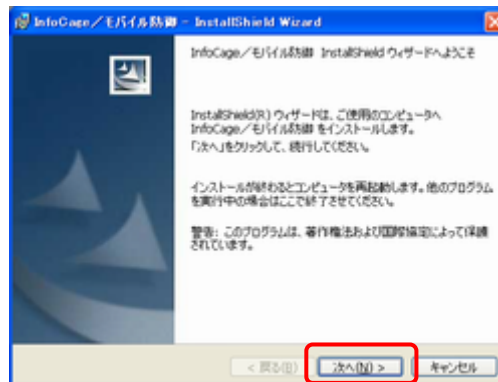
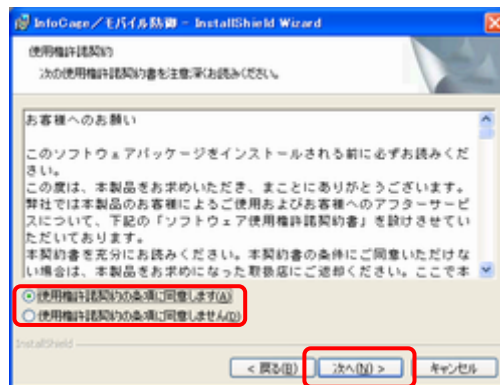
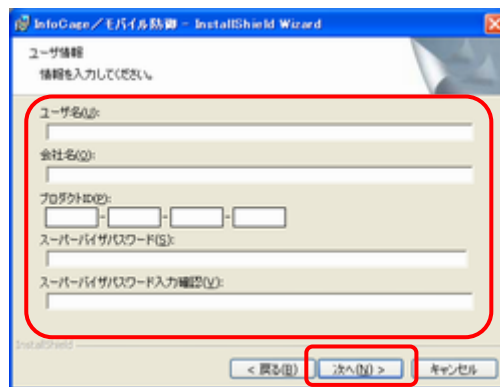
Operation

1. InfoCage モバイル防御が格納されているメディア (例 CD-ROM) 内の setup.exe を実行し、「次へ」をクリックしてください。

2. 『「メディア鍵認証方式の InfoCage モバイル防御」をインストール』または『「パスワード認証方式の InfoCage モバイル防御」をインストール』のいずれかを選択し、「次へ」をクリックしてください。

   * InfoCage モバイル防御の管理者によって運用形態が設定されている場合は、この画面は表示されません。

   * アップグレードの場合、「アップグレードインストールを行います」と表示されますので、「次へ」をクリックし、「続行しますか？」と表示されましたら「はい」をクリックしてください。

3. 「導入前の注意事項」 画面が表示されます。
各項目をクリックすると詳細な説明が表示されますので、必ずお読みの上、チェックを付けてください。
すべての確認が終わりましたら、「閉じる」をクリックしてください。

* 画面はメディア鍵認証方式の場合です。パスワード認証方式の場合は一部異なります。

4. すべての項目がチェックされていない場合は、下記のメッセージが表示されます。
インストールを続ける場合は「はい」を、インストールを中止する場合は「いいえ」を、*3* の画面に戻る場合は「キャンセル」をクリックしてください。

5. 「次へ」をクリックしてください。

6. 使用権許諾契約をすべてお読みいただき、同意する場合は「使用権許諾の条項に同意します」をクリックしてください。
「使用権許諾の条項に同意しません」を選択した場合はインストールできません。

7. ユーザ情報を入力します。
ユーザ名、会社名、プロダクトID、スーパーバイザパスワード／ユーザパスワードを入力します。
(確認のため、スーパーバイザパスワード／ユーザパスワードは2回入力してください。)
すべての入力が終わりましたら、「次へ」をクリックしてください。

ユーザ名、会社名	半角40文字以内、または全角20文字以内で入力してください。
プロダクトID	ライセンス証書に記載されているものを半角文字で入力してください。 (大文字小文字は区別しません)。
スーパーバイザパスワード	8文字以上64文字以内の半角英数および記号を指定してください。 (大文字小文字を区別します)。
ユーザパスワード	8文字以上32文字以内の半角英数および記号を指定してください。 (大文字小文字を区別します)

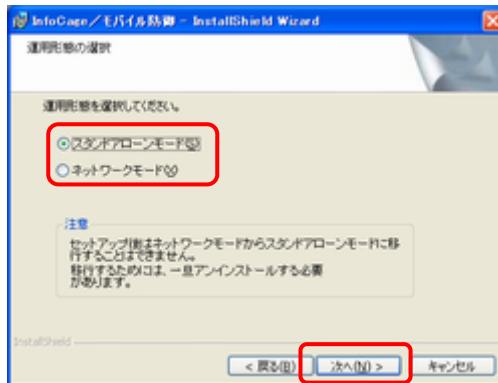
* 画面はメディア鍵認証方式版です。パスワード認証方式版の場合は、「スーパーバイザパスワード」の欄は「ユーザパスワード」と表示されます。

* スーパーバイザパスワード／ユーザパスワードとはInfoCage モバイル防御ユーティリティを起動するときなどに必要なパスワードです。忘れないよう注意してください。

8. 「運用形態の選択」 画面で、運用形態の選択をします。

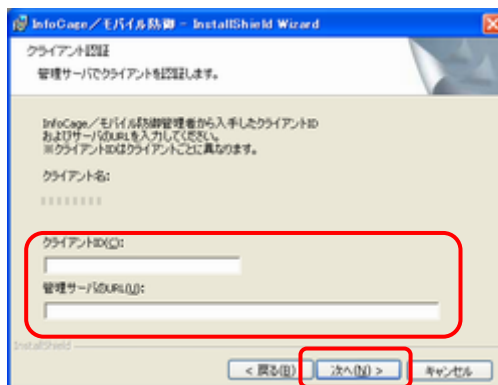
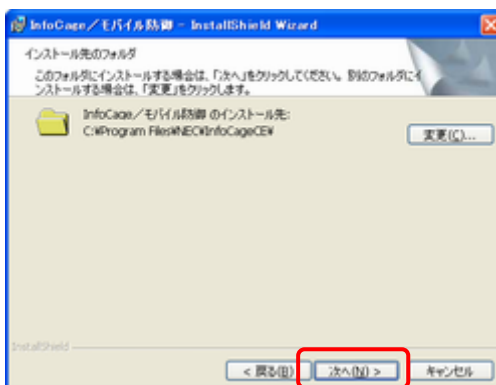
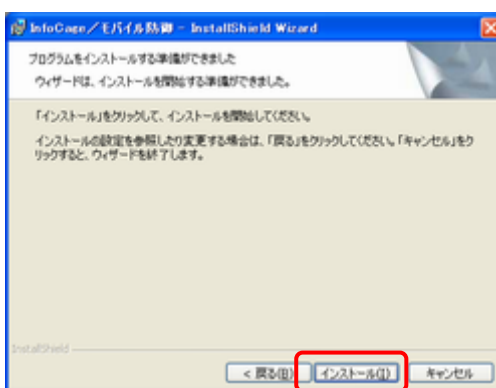
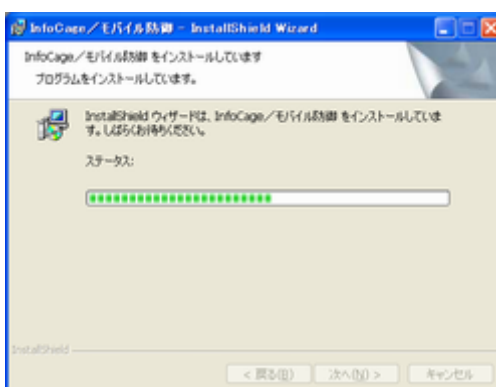
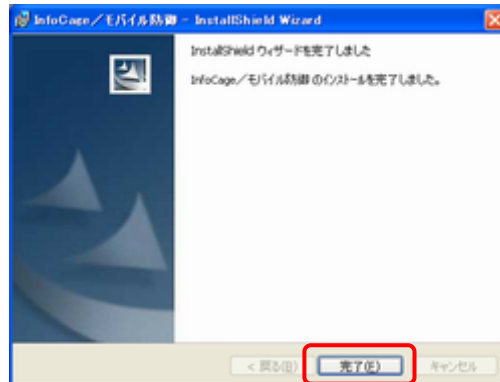
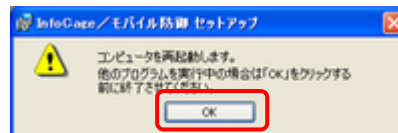
* 別売の InfoCage モバイル防御 管理サーバが導入されていない環境では、スタンドアローンモードを選択してください。
InfoCage モバイル防御管理サーバが導入されている環境では、InfoCage モバイル防御の管理者に問い合わせて運用形態を選択してください。

* InfoCage モバイル防御の管理者によって運用形態が設定されている場合は、この画面は表示されません。

* スタンドアローンモードを選択した場合は *10* へ進んでください。

9. ≪ネットワークモード≫を選択した場合、クライアント認証画面が表示されるので、クライアント ID、管理サーバの URL を入力して、「次へ」をクリックしてください。

* スタンドアローンモードの場合、この画面は表示されません。

* 認証に失敗した場合は、クライアント名、クライアント ID、管理サーバの URL を確認後、InfoCage モバイル防御の管理者に問い合わせてください。

* InfoCage モバイル防御の管理者がクライアント登録をしていない場合は認証されません。

10. インストール先のフォルダ選択画面で InfoCage モバイル防御のインストールフォルダを選択します。通常はそのまま「次へ」をクリックしてください。

11. 「インストール」をクリックしてインストールを開始してください。

12. インストール中です。しばらくお待ちください。

13. インストールが完了すると下記の画面が表示されます。
「完了」をクリックしてください。

14. InfoCage モバイル防御を使用可能にするためには、パソコンを再起動する必要があります。
他のプログラムを実行中の場合は、終了させてください。
「OK」をクリックすると、パソコンが再起動します。

続いて本ガイドの「3.2 Step」へ進み、それぞれの認証方式の項を参照してください。

3.2.1　　メディア鍵認証方式の場合
3.2.2　　パスワード認証方式の場合

InfoCage モバイル防御の管理者の設定により、個別暗号モードでインストールした場合は、「第 4 章 個別暗号モードインストール」へ進んでください。

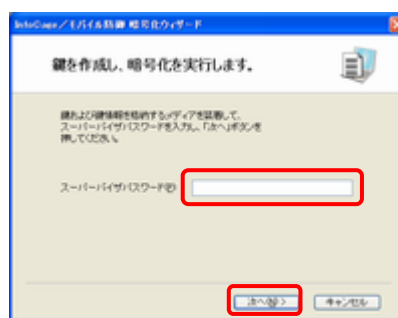
3.2　Step2

再起動後、暗号化ウィザードが起動します。
それぞれの認証方式の説明にしたがって、暗号化を行ってください。

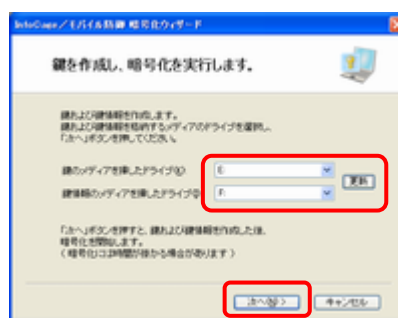
* 何らかの理由で暗号化ウィザートを終了させた場合、再度暗号化ウィザードを起動するには、スタートメニューから［すべてのプログラム］－[NEC]－[InfoCage／モバイル防御]－[InfoCage／モバイル防御　ユーティリティ］をクリックします。

3.2.1　メディア鍵認証方式の場合

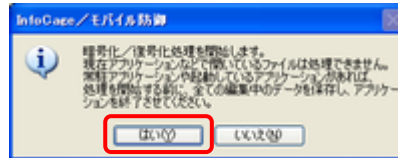
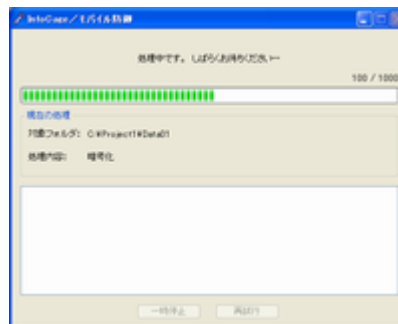
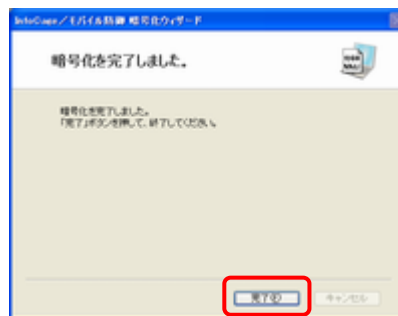
Operation

1. 鍵を格納するメディアと鍵情報を格納するメディアを装着し、インストール時に設定したスーパーバイザパスワードを入力して「次へ」をクリックしてください。

* 他のパソコンの InfoCage モバイル防御 ユーティリティまたはメディア暗号ユーティリティで暗号化したリムーバブルメディアは、暗号化を実行する前に必ず抜いてください。
装着したまま暗号化を開始すると上図と異なる画面が表示されますので、一旦「キャンセル」をクリックし、リムーバブルメディアを抜いてから再度暗号化ウィザードを起動してください。

2. 鍵および鍵情報を作成します。
鍵を格納するメディア　および　鍵情報を格納するメディアのドライブを選択してください。
格納するメディアが表示されないときは、「更新」をクリックします。
「次へ」をクリックしてください。

* InfoCage モバイル防御の管理者によりあらかじめ鍵および鍵情報の格納先が設定されている場合は下記の画面が異なります。

3. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。

* アプリケーションが使用しているファイルは、暗号化できない場合があります。
* 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
またゴミ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、ゴミ箱を空にしておくことをお勧めします。

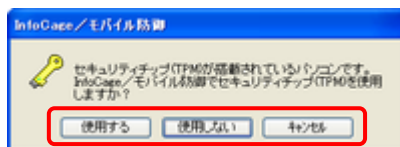
「はい」をクリックすると暗号化が開始されます。

4. 暗号化処理中です。しばらくお待ちください。

5. 暗号化を完了しました。
「完了」をクリックしてください。

6. 以上で暗号化は完了しました。

その他の設定については、「InfoCage/モバイル防御 ユーザーズガイド」を参照してください。

* この段階では、Program Files やアプリケーションのインストールフォルダ以下は暗号化されていません。
Program Files やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、「InfoCage/モバイル防御 ユーザーズガイド」の「アプリケーションのフォルダを暗号化指定する」の項を参照してください。

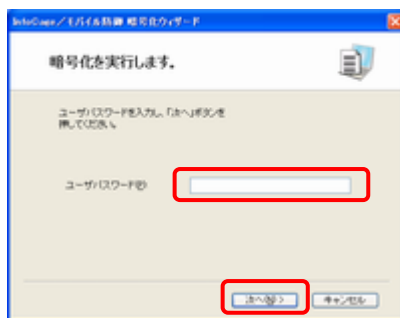
3.2.2　パスワード認証方式の場合

● **セキュリティチップ (TPM) 搭載のパソコンをお使いでセキュリティチップ (TPM) が有効になっている場合**

InfoCage モバイル防御の管理者の設定によっては、再起動後にユーザパスワードを入力して Windows にログオンすると、下記の画面が表示される場合があります。

セキュリティチップ (TPM) を使用する場合は「使用する」を、使用しない場合は「使用しない」を、後で選択する場合は「キャンセル」をクリックしてください。
「キャンセル」をクリックした場合、TPM の使用を選択するまで InfoCage モバイル防御 ユーティリティの起動時にメッセージが表示されます。

* セキュリティチップ (TPM) に関しては、「第 10 章 セキュリティチップ (TPM) 搭載のパソコンをお使いの場合」を参照してください。

● **ログオン認証にパスワードを使用する場合**

1. インストール時に設定した InfoCage モバイル防御のユーザパスワードを入力して Windows にログオンすると、下記の画面が表示されます。
ユーザパスワードを入力して「次へ」をクリックしてください。

* 他のパソコンの InfoCage モバイル防御 ユーティリティまたはメディア暗号ユーティリティで暗号化したリムーバブルメディアは、暗号化を実行する前に必ず抜いてください。
装着したまま暗号化を開始すると上図と異なる画面が表示されますので、一旦「キャンセル」をクリックし、リムーバブルメディアを抜いてから再度スタートメニューから［すべてのプログラム］－[NEC]－[InfoCage／モバイル防御]－[InfoCage／モバイル防御 ユーティリティ]をクリックし、暗号化ウィザードを起動して操作してください。

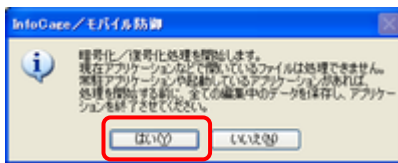
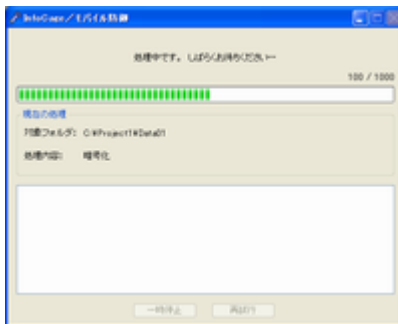
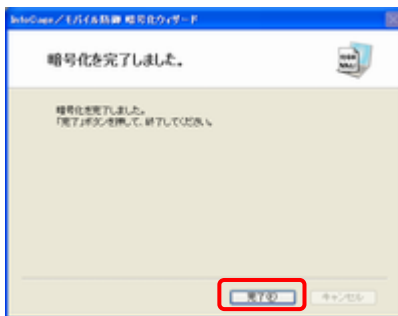
2. 暗号化を実行します。「次へ」をクリックしてください。

＊ 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

3. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。

＊ アプリケーションが使用しているファイルは、暗号化できない場合があります。

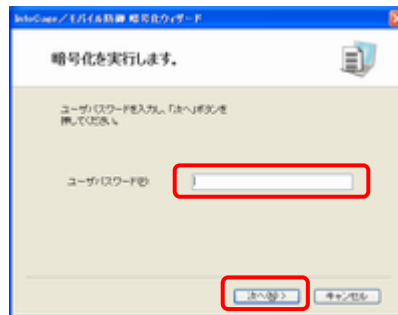
＊ 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
またゴミ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、ゴミ箱を空にしておくことをお勧めします。

「はい」をクリックすると暗号化が開始されます。

4. 暗号化処理中です。しばらくお待ちください。

5. 暗号化を完了しました。
「完了」をクリックしてください。

6. 以上でインストールは完了しました。

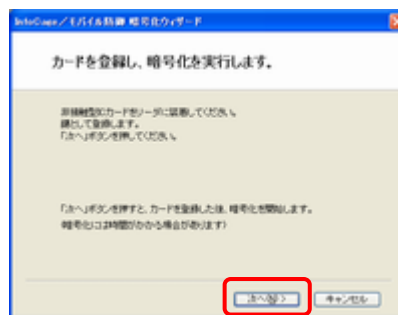
その他の設定については、「InfoCage/モバイル防御 ユーザーズガイド」を参照してください。

* この段階では、Program Files やアプリケーションのインストールフォルダ以下は暗号化されていません。Program Files やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、「InfoCage/モバイル防御 ユーザーズガイド」の「アプリケーションのフォルダを暗号化指定する」の項を参照してください。

● **ログオン認証に FeliCa カードを使用する場合**

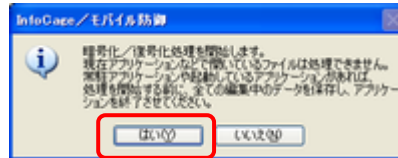
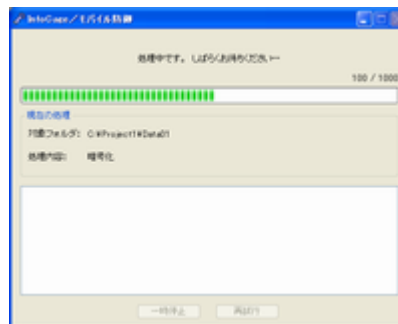
1. インストール時に設定した InfoCage モバイル防御のユーザパスワードを入力して Windows にログオンすると、下記の画面が表示されます。
ユーザパスワードを入力して「次へ」をクリックしてください。

* 他のパソコンの InfoCage モバイル防御 ユーティリティまたはメディア暗号ユーティリティで暗号化したリムーバブルメディアは、暗号化を実行する前に必ず抜いてください。
装着したまま暗号化を開始すると上図と異なる画面が表示されますので、一旦「キャンセル」をクリックし、リムーバブルメディアを抜いてから再度スタートメニューから[すべてのプログラム]－[NEC]－[InfoCage／モバイル防御]－[InfoCage／モバイル防御 ユーティリティ]をクリックし、暗号化ウィザードを起動して操作してください。

2. FeliCa カードをカードリーダにセットして「次へ」をクリックしてください。

* FeliCa のカードリーダを使用可能な状態にしてから操作してください。

3. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。

* アプリケーションが使用しているファイルは、暗号化できない場合があります。

* 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
またゴミ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、ゴミ箱を空にしておくことをお勧めします。

「はい」をクリックすると暗号化が開始されます。

4. 暗号化処理中です。しばらくお待ちください。

5. 暗号化を完了しました。
「完了」をクリックしてください。

6. 以上でインストールは完了しました。

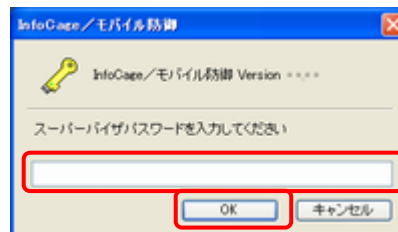
その他の設定については、「InfoCage/モバイル防御　ユーザーズガイド」を参照してください。

* この段階では、Program Files やアプリケーションのインストールフォルダ以下は暗号化されていません。
Program Files やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、「InfoCage/モバイル防御　ユーザーズガイド」の「アプリケーションのフォルダを暗号化指定する」の項を参照してください。

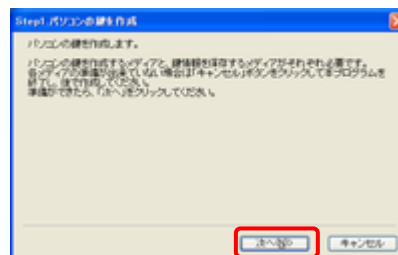
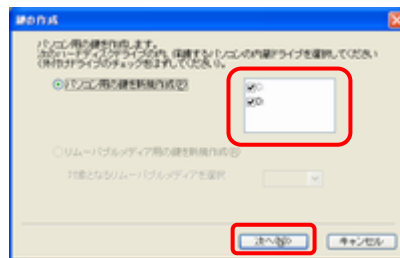
第4章　個別暗号モードインストール

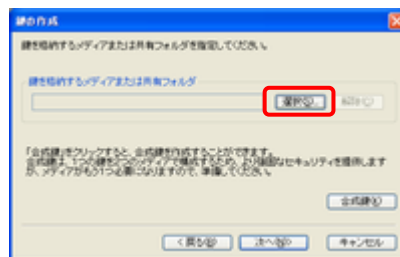
InfoCage モバイル防御は、インストール後の暗号化モード（ドライブ一括暗号モード または 個別暗号モード）を InfoCage モバイル防御の管理者により設定することができます。
暗号化モードを「個別暗号モード」に設定した場合、「3.1 Step1」のインストールを完了し再起動した後は、本章にしたがって操作してください。

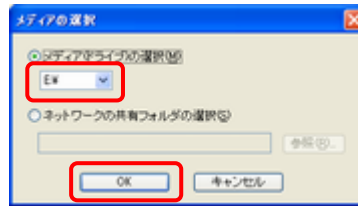
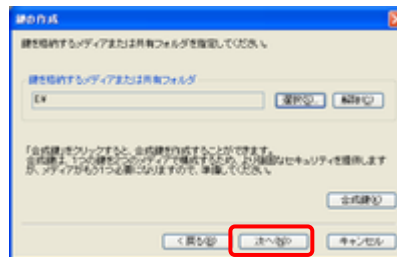
4.1　メディア鍵認証方式の場合

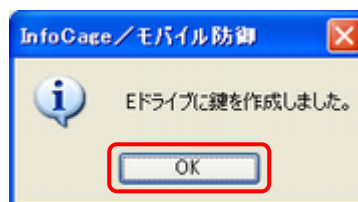
1. 再起動後に、スーパーバイザパスワード入力画面が表示されます。インストール時に設定したスーパーバイザパスワードを入力し、「OK」をクリックしてください。

2. 設定のご案内が表示されます。「次へ」をクリックしてください。

* 「キャンセル」をクリックすると、本プログラムが終了します。その場合は、後でパソコンの鍵を作成してください。

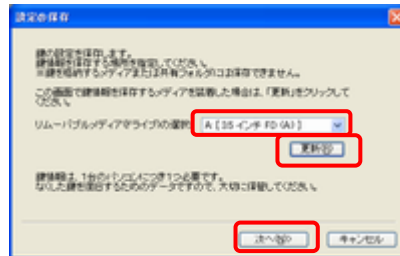
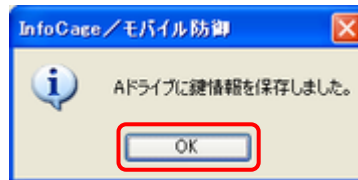
3. パソコンの鍵の作成に関する説明が表示されます。
必ずお読みの上、準備ができましたら、「次へ」をクリックしてください。

4. 「パソコン用の鍵を新規作成」が選択されています。ドライブ一覧に、内蔵ハードディスクドライブ以外のドライブが表示されている場合はチェックをはずしてください。
鍵を作成するメディアを装着し、「次へ」をクリックしてください。

* システムドライブのチェックは外せません。
* 内蔵ハードディスクドライブは必ずチェックしてください。
内蔵ハードディスクドライブのチェックを外すと、その内蔵ハードディスクドライブへのデータのコピー、移動およびファイルの新規作成ができなくなったり、その内蔵ハードディスクドライブにインストールされたアプリケーションが正しく動作しなくなったりする場合があります。
* 内蔵ハードディスクドライブではないドライブのチェックは必ずはずしてください。
内蔵ハードディスクドライブではないドライブにチェックをつけると、そのドライブを取り外した際に動作が不正になる場合があります。

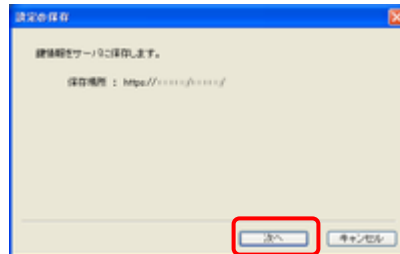
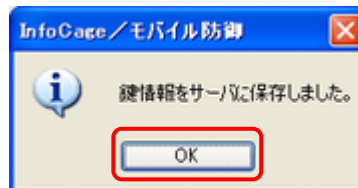
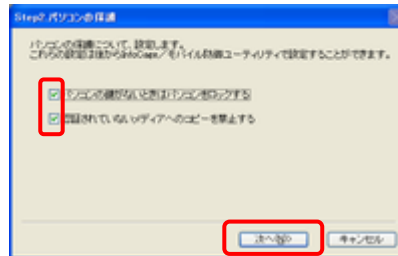
5. 「鍵を格納するメディアまたは共有フォルダ」の「選択」をクリックしてください。
(以下では一つの鍵を作成する方法を説明します)

* 合成鍵を作成する場合は、「InfoCage/モバイル防御 ユーザーズガイド」の「合成鍵を作成する」の項を参照してください。

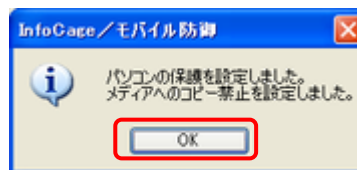
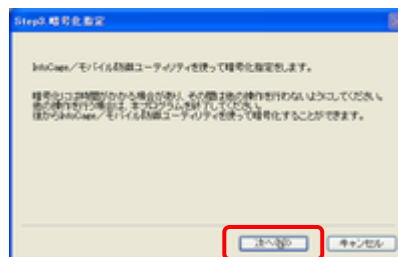
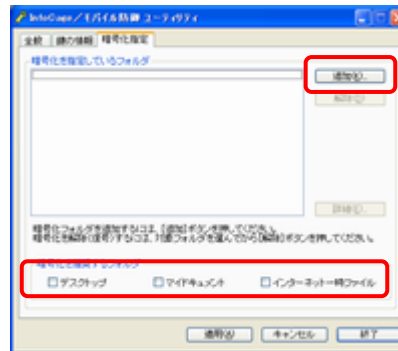
6. 「メディア（ドライブ）の選択」をクリックして選択し、ドライブ一覧から鍵を作成するメディアのドライブを選択してください。（ここでは例として E ドライブとします）
ドライブ指定後、「OK」をクリックしてください。

7. 「次へ」をクリックしてください。

8. 作成内容を確認後、「作成」をクリックしてください。

9. 鍵の作成が完了しました。「OK」をクリックしてください。

10. 続いて鍵情報を保存します。

● スタンドアローンモードの場合

鍵情報を保存するリムーバブルメディアを装着してください。
（ここでは例としてフロッピーディスクに保存します）
リムーバブルメディア（ドライブ）一覧に鍵情報を保存するメディアが見つからない場合は、「更新」をクリックしてください。
鍵情報の保存先メディアを選択し、「次へ」をクリックしてください。

鍵情報の保存が完了しました。「OK」をクリックしてください。

● ネットワークモードの場合

鍵情報をサーバに保存します。保存場所を確認して、「次へ」をクリックしてください。

鍵情報の保存が完了しました。「OK」をクリックしてください。

11. パソコンの保護に関する設定画面が表示されます。
あらかじめ「パソコンの鍵がないときはパソコンをロックする」にチェックが入っています。
データの抜き取り防止設定をする場合は、「認証されていないメディアへのコピーを禁止する」のチェックを入れて「次へ」をクリックしてください。

* 通常は「パソコンの鍵がないときはパソコンをロックする」のチェックを入れて使用してください。
このチェックを外す場合は、「InfoCage/モバイル防御 ユーザーズガイド」の「パソコンのロック」の項を参照してください。
* InfoCage モバイル防御の管理者の設定により外部メディア自動暗号が有効になっている場合、「認証されていないメディアへのコピーを禁止する」はチェックできない場合があります。

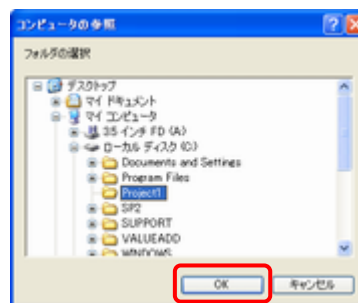
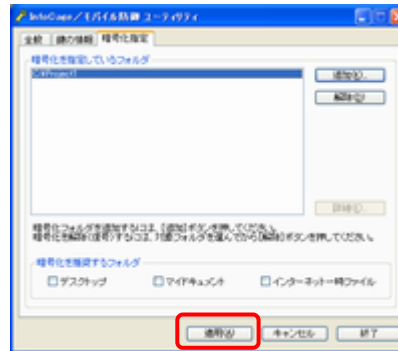
12. 「OK」をクリックしてください。パソコンをロックする設定が有効になります。
これ以降、認証されていないメディアへのコピーを禁止します。また、鍵を抜くと、パソコンをロックします。
鍵を装着するとロックが解除され、ログオンすることができます。

13. 暗号化指定に関する説明が表示されます。
必ずお読みの上、準備ができましたら、「次へ」をクリックしてください。

14. 「暗号化指定」タブが表示されます。「追加」をクリックしてください。

以下のフォルダを暗号化する場合は、「暗号化を推奨するフォルダ」内のチェックボックスにチェックを入れてください。

・デスクトップ　　　・マイドキュメント　　　・インターネット一時ファイル

* デスクトップを暗号化または復号した場合、デスクトップの表示が不正になる場合があります。その場合はデスクトップの任意の場所をクリックし、「F5」キーを押すと正常に戻ります。また、アイコンの並びが変更される場合がありますが、その場合は手動で並び替えてください。

* InfoCage モバイル防御　管理サーバが導入されている環境で、InfoCage モバイル防御の管理者によって暗号化するドライブやフォルダがあらかじめ設定されている場合は、そのドライブやフォルダが「暗号化を指定しているフォルダ」に表示されています。

他に暗号化設定するドライブやフォルダがない場合は、*16* へ。

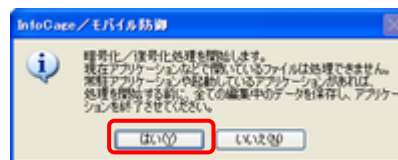
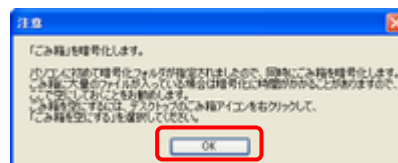
15. 暗号化したいフォルダを選択し、「OK」をクリックしてください。

16. 「暗号化を指定しているフォルダ」に選択したフォルダが追加されます。
複数のフォルダを指定したい場合は、14 ～ 15 を繰り返してください。

すでに暗号化したドライブやフォルダがある場合、そのドライブやフォルダ名も表示されていますが、「解除」すると復号されますのでご注意ください。

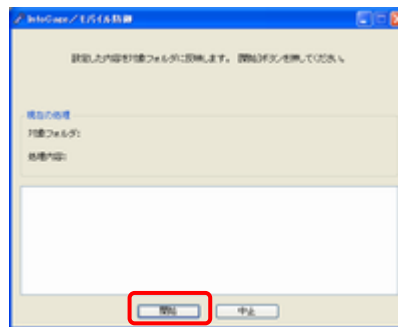
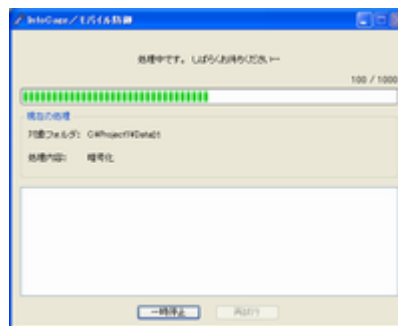
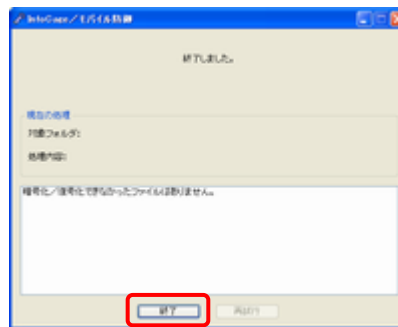
* 「適用」をクリックすると、暗号化処理が終了するまで暗号化指定しているフォルダにはアクセスできなくなります。（「一時停止」をクリックしても同様です）

全て指定し終わったら「適用」をクリックしてください。

* ここで「終了」をクリックすると、指定したフォルダの暗号化を実行後に、InfoCage モバイル防御ユーティリティが終了します。

17. 暗号化処理に関する注意事項が表示されます。常駐アプリケーションや起動しているアプリケーションがあれば終了し、「はい」をクリックしてください。

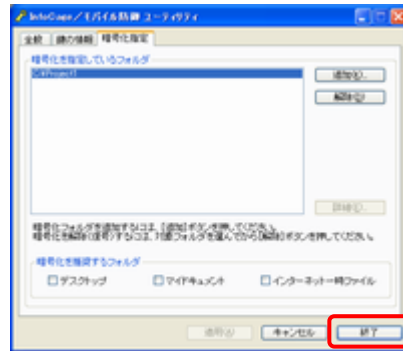
* 暗号化を実行する前に、常駐プログラムを含むすべてのアプリケーションを必ず終了させてください。アプリケーションが使用しているファイルは、暗号化できない場合があります。

18. ごみ箱の暗号化に関する注意事項が表示されます。必ずお読みの上、「OK」をクリックしてください。

19. 「開始」をクリックすると、暗号化処理が始まります。

* 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

20. 暗号化処理中です。しばらくお待ちください。

21. 暗号化処理が終了しました。
暗号化できなかったファイルがある場合はウィンドウ内に表示されます。

「終了」をクリックしてください。

* 暗号化できなかったファイルがあった場合は、起動しているアプリケーションがあれば終了し、「再試行」をクリックしてください。
すべての起動中のアプリケーションを終了して「再試行」をクリックしても暗号化できなかったファイルがある場合、そのファイルはオペレーティングシステムのサービス等で優先的に使用されているため、暗号化できません。
これらのファイルは本ソフトウェア内で暗号化できなかったファイルとして登録されるため、暗号化対象フォルダ内にあっても、問題はありません。

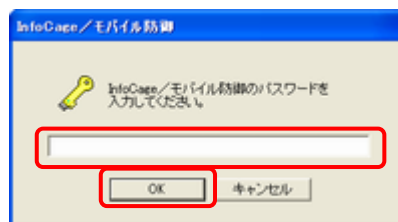
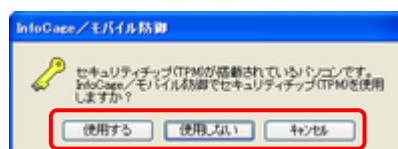
* 暗号化対象外ファイルについては、暗号化できなかったファイルの一覧には表示されません。
また、暗号化対象フォルダ内の全てのファイルが暗号化対象外ファイルであった場合は、「処理したファイルはありませんでした」と表示されます。

* 暗号化対象外ファイルについては、「InfoCage／モバイル防御　ユーザーズガイド」の「「暗号化指定」タブ　」の項を参照してください。

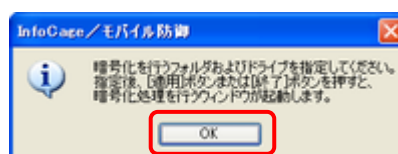
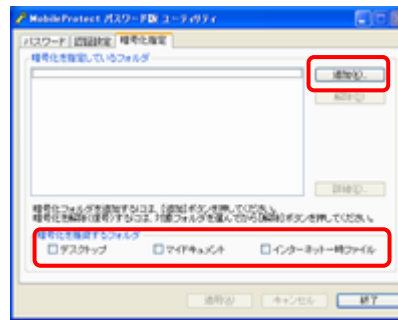
22. 「暗号化を指定しているフォルダ」に暗号化されたフォルダが表示されます。
これで暗号化の作業は終了です。「終了」をクリックしてください。

その他の設定に関しては、「InfoCage/モバイル防御 ユーザーズガイド」を参照してください。

4.2　パスワード認証方式の場合

Operation

1. 再起動後に、ユーザパスワード入力画面が表示されます。インストール時に設定したユーザパスワードを入力し、Windows へログオンしてください。

2. セキュリティチップ（TPM）搭載のパソコンをお使いでセキュリティチップ（TPM）が有効になっている場合、InfoCage モバイル防御の管理者の設定によっては、下記の画面が表示される場合があります。

セキュリティチップ（TPM）を使用する場合は「使用する」を、使用しない場合は「使用しない」を、後で選択する場合は「キャンセル」をクリックしてください。
「キャンセル」をクリックした場合、TPM の使用を選択するまで InfoCage モバイル防御ユーティリティの起動時にメッセージが表示されます。

＊ セキュリティチップ（TPM）に関しては、本ガイドの「第 10 章 セキュリティチップ（TPM）搭載のパソコンをお使いの場合」を参照してください。

3. 初回起動時、Windows にログオンすると、自動で InfoCage モバイル防御ユーティリティが起動します。
暗号化処理に関する説明が表示されますので、必ずお読みの上、「OK」をクリックしてください。

4. 「暗号化指定」タブが表示されています。「追加」をクリックしてください。

以下のフォルダを暗号化する場合は、「暗号化を推奨するフォルダ」内のチェックボックスにチェックを入れてください。

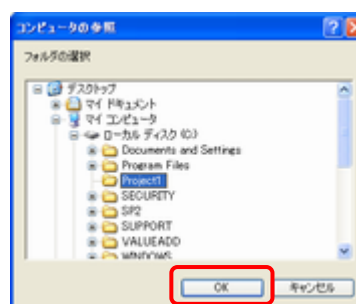
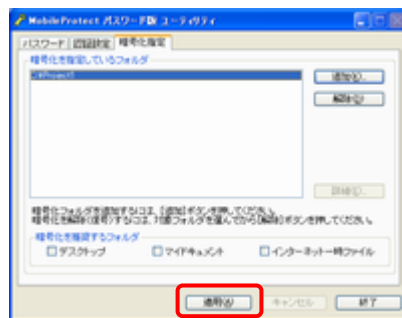
・ デスクトップ　　・ マイドキュメント　・ インターネット一時ファイル

* InfoCage モバイル防御の管理者の設定により外部メディア自動暗号機能が有効の場合、システムドライブを除く暗号化フォルダの指定がない内蔵ハードディスクドライブは、リムーバブルメディアと同じ扱いとなり、その内蔵ハードディスクドライブへはデータのコピー、移動およびファイルの新規作成ができなくなります。また、その内蔵ハードディスクドライブにインストールされたアプリケーションが正しく動作しない場合がありますので、すべての内蔵ハードディスクドライブに暗号化フォルダを作成してください。

* デスクトップを暗号化または復号した場合、デスクトップの表示が不正になる場合があります。その場合はデスクトップの任意の場所をクリックし、「F5」キーを押すと正常に戻ります。また、アイコンの並びが変更される場合がありますが、その場合は手動で並び替えてください。

* 管理サーバが導入されている環境で、InfoCage モバイル防御の管理者によって暗号化するドライブやフォルダがあらかじめ設定されている場合は、そのドライブやフォルダが「暗号化を指定しているフォルダ」に表示されています。

他に暗号化設定するドライブやフォルダがない場合は、*6* へ。

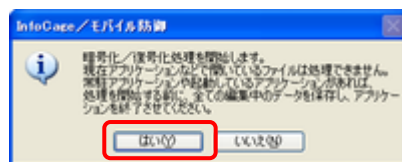
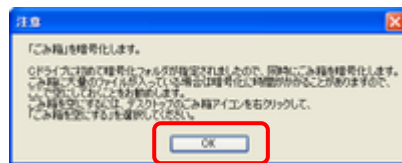
5. 暗号化したいフォルダを選択し、「OK」をクリックしてください。

6. 「暗号化を指定しているフォルダ」に選択したフォルダが追加されます。
複数のフォルダを指定したい場合は、*4* ～ *5* を繰り返してください。

すでに暗号化したドライブやフォルダがある場合、そのドライブやフォルダ名も表示されていますが、「解除」すると、復号されるためご注意ください。

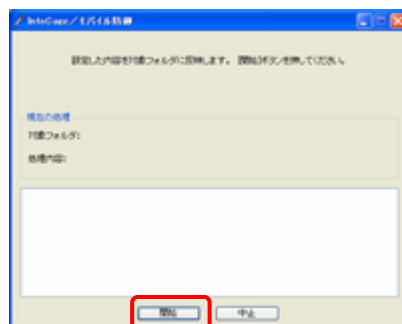
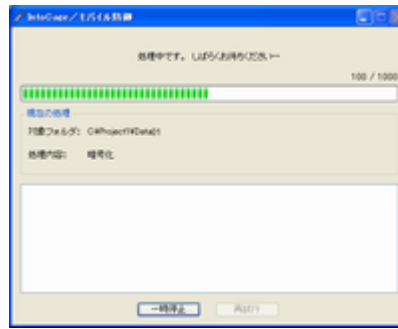
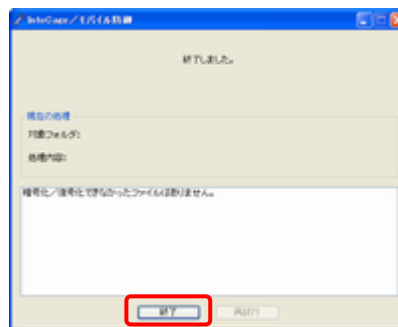
* 暗号化を実行する前に、常駐プログラムを含むすべてのアプリケーションを必ず終了させてください。
アプリケーションが使用しているファイルは、暗号化できない場合があります。

* 「適用」をクリックすると、暗号化処理が終了するまで暗号化指定しているフォルダにはアクセスできなくなります。（「一時停止」をクリックしても同様です）
全て指定し終わったら「適用」をクリックしてください。

* ここで「終了」をクリックすると、指定したフォルダの暗号化を実行後に、InfoCage モバイル防御ユーティリティが終了します。

7. 暗号化処理に関する注意事項が表示されます。必ずお読みの上、「はい」をクリックしてください。

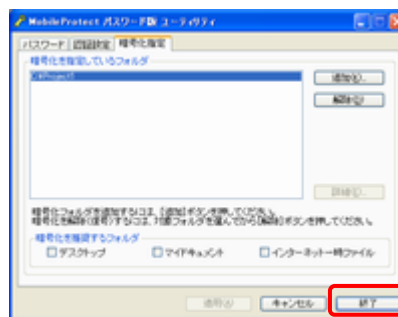
* 暗号化を実行する前に、常駐プログラムを含むすべてのアプリケーションを必ず終了させてください。
アプリケーションが使用しているファイルは、暗号化できない場合があります。

8. ごみ箱の暗号化に関する注意事項が表示されます。必ずお読みの上、「OK」をクリックしてください。

9. 「開始」をクリックすると、暗号化処理が始まります。

* 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

10. 暗号化処理中です。しばらくお待ちください。

11. 暗号化処理が終了しました。
暗号化できなかったファイルがある場合はウィンドウ内に表示されます。

「終了」をクリックしてください。

* 暗号化できなかったファイルがあった場合は、起動しているアプリケーションがあれば終了し、「再試行」をクリックしてください。
すべての起動中のアプリケーションを終了して「再試行」をクリックしても暗号化できなかったファイルがある場合、そのファイルはオペレーティングシステムのサービス等で優先的に使用されているため、暗号化できません。
これらのファイルは本ソフトウェア内で暗号化できなかったファイルとして登録されるため、暗号化対象フォルダ内にあっても、問題はありません。

* 暗号化対象外ファイルについては、暗号化できなかったファイルの一覧には表示されません。
また、暗号化対象フォルダ内の全てのファイルが暗号化対象外ファイルであった場合は、「処理したファイルはありませんでした」と表示されます。

* 暗号化対象外ファイルについては、「InfoCage/モバイル防御 ユーザーズガイド」の「「暗号化指定」タブ 」の項を参照してください。

12. 暗号化を指定しているフォルダ」に暗号化されたフォルダが表示されます。
これで暗号化の作業は終了です。「終了」をクリックしてください。

その他の設定に関しては、「InfoCage/モバイル防御 ユーザーズガイド」を参照してください。

第5章　アップグレードインストール

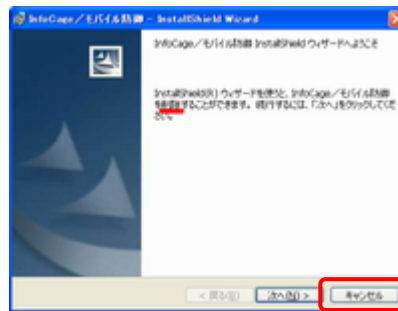
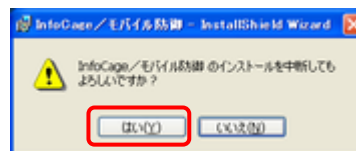
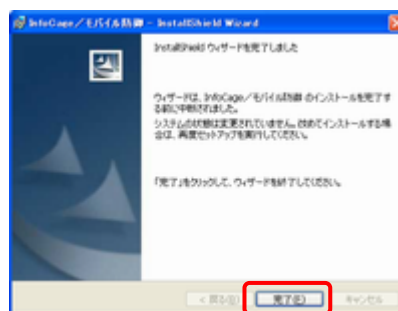
注意

アップグレードインストールを行う前に、InfoCage モバイル防御を使用するパソコンの環境をチェックしてください。
（環境のチェック方法）
InfoCage モバイル防御が格納されているメディア（例 CD-ROM）内の¥2K_XP¥Tools¥環境チェックUPG¥MPEnvChkUpg.EXEを実行してください。
問題が見つかった場合は、すべて対処してください。画面内の「対処方法」をクリックすると、対処方法が表示されます。

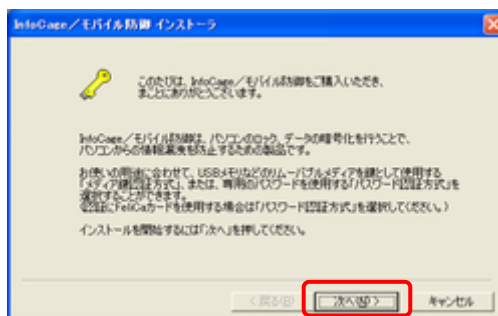
注意

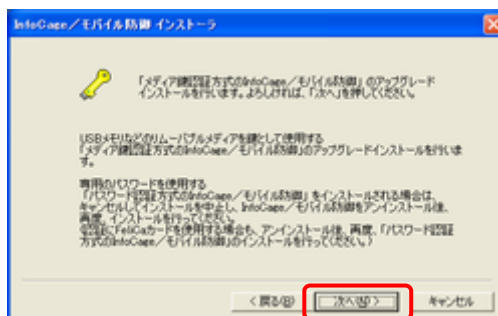
既にインストールされているInfoCage モバイル防御と同じバージョンのsetup.exeを実行するとアンインストールのウィザードが起動しますのでご注意ください。
その際は下記の手順にしたがって操作してください。

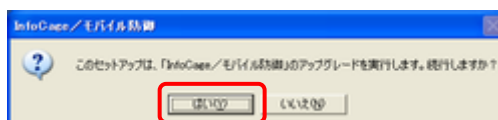
Operation

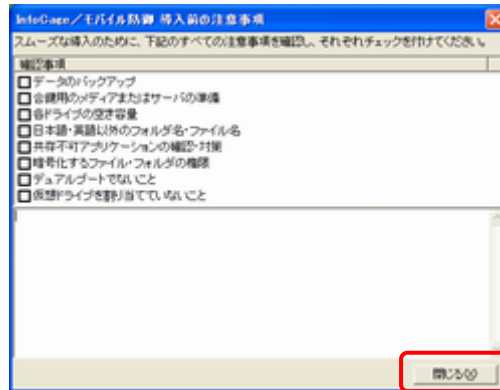
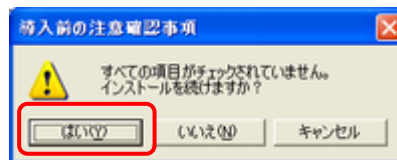
1. setup.exe を実行すると、「InstallShield(R)ウィザードを使うと、InfoCage モバイル防御を削除することができます。」と表示された場合は、「キャンセル」をクリックしてください。

2. 「はい」をクリックしてください。

3. 「完了」をクリックしてください。操作は以上です。

アップグレードインストールを行います。

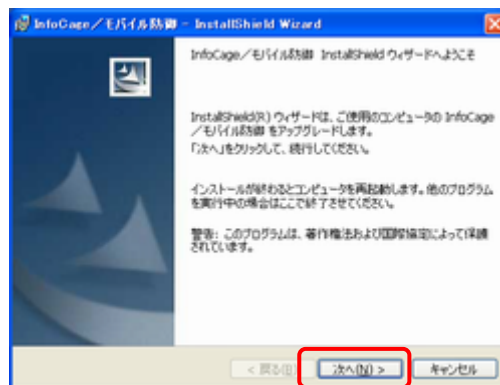
Operation

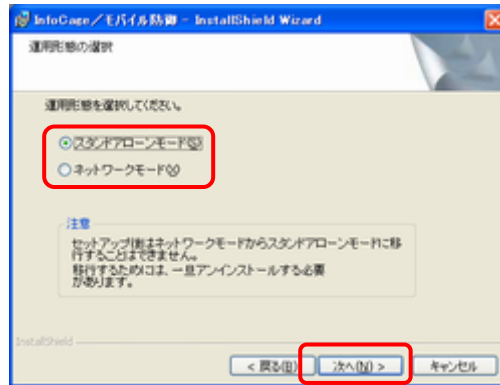
1. InfoCage/モバイル防御が格納されているメディア（例 CD-ROM）内の setup.exe を実行し、「次へ」をクリックしてください。

2. インストールする InfoCage/モバイル防御のプログラムの確認画面が表示されます。「次へ」をクリックしてください。

   * 画面はメディア鍵認証方式版です。

3. 確認メッセージが表示されます。「はい」をクリックしてください。

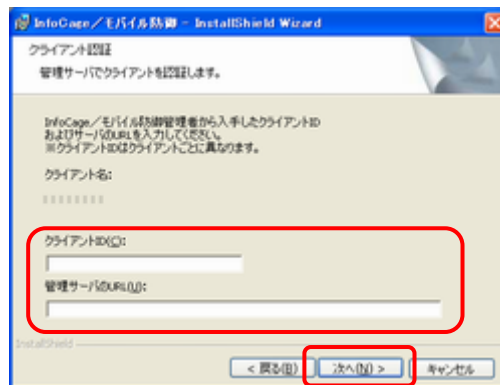
   * アップグレードする InfoCage モバイル防御のバージョンによっては、この画面は表示されません。

4. 「導入前の注意事項」 画面が表示されます。
各項目をクリックすると詳細な説明が表示されますので、必ずお読みの上、チェックを付けてください。
すべての確認が終わりましたら、「閉じる」をクリックしてください。

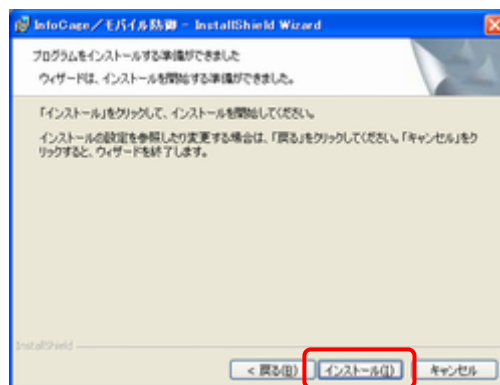
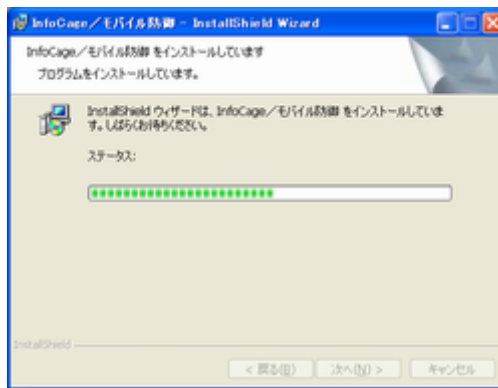
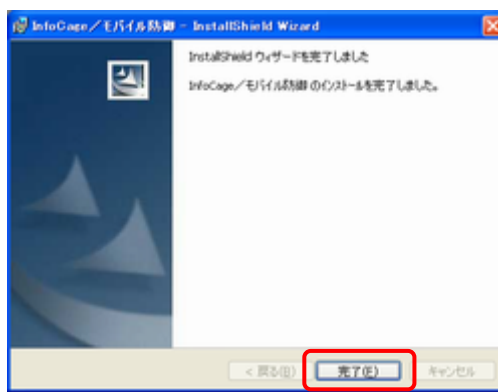
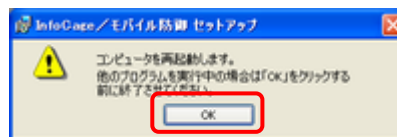
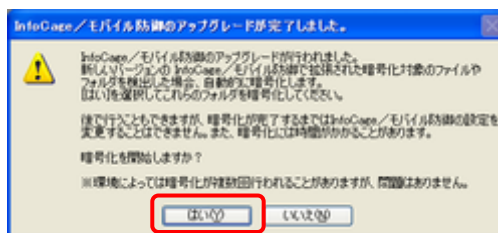
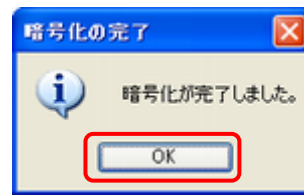
* 画面はメディア鍵認証方式の場合です。パスワード認証方式の場合は一部異なります。

5. すべての項目がチェックされていない場合は、下記のメッセージが表示されます。
インストールを続ける場合は「はい」を、インストールを中止する場合は「いいえ」を、**4** の画面に戻る場合は「キャンセル」をクリックしてください。

6. 「次へ」をクリックしてください。

* お使いのバージョンによっては「InfoCage モバイル防御用の InstallShield ウィザードを続行しています」と表示されますので、**7** または**9** または**10** へ進みます。

7. 「運用形態の選択」 画面で、運用形態の選択をします。

* アップグレードする InfoCage モバイル防御のバージョンによっては、この画面は表示されません。

* スタンドアローンモードを選択した場合は *9* へ。

8. ≪ネットワークモード≫を選択した場合、クライアント認証画面が表示されるので、クライアント ID、管理サーバの URL を入力して、「次へ」をクリックしてください。

* アップグレードする InfoCage モバイル防御のバージョンによっては、この画面は表示されません。
* スタンドアローンモードの場合、この画面は表示されません。

* 認証に失敗した場合は、クライアント名、クライアント ID、管理サーバの URL を確認後、InfoCage モバイル防御の管理者に問い合わせてください。
* InfoCage モバイル防御の管理者がクライアント登録をしていない場合は認証されません。

9. 「インストール」をクリックしてインストールを開始してください。

10. インストール中です。しばらくお待ちください。

11. インストールが完了すると下記の画面が表示されます。「完了」をクリックしてください。

12. InfoCage モバイル防御を使用可能にするためには、パソコンを再起動する必要があります。
他のプログラムを実行中の場合は、終了させてください。
「OK」をクリックすると、パソコンが再起動します。

13. お使いのバージョンによっては、再起動後に表示されるパスワード入力画面でスーパーバイザ
パスワード／ユーザパスワードを入力すると、下記のメッセージが表示される場合があります。
必ずお読みの上、「はい」をクリックしてください。
暗号化を後で行う場合は「いいえ」をクリックしてください。
「いいえ」をクリックした場合、暗号化が完了するまでは InfoCage モバイル防御 ユーティリティを起動する
ごとにメッセージが表示されます。

14. 暗号化が完了すると下記のメッセージが表示されますので、「OK」をクリックし、InfoCage モバイル防御ユーティリティを終了してください。

以上で操作は完了です。

第6章　ログオン方法

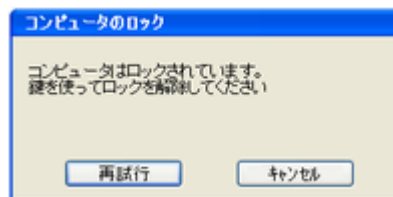
6.1　　メディア鍵認証方式の場合

（画面イメージは Windows XP　Professional です）

● **起動しているパソコンから鍵を抜いた場合**

起動しているパソコンから鍵を抜くと、「コンピュータのロック」画面が表示され、パソコンがロックされた状態になります。

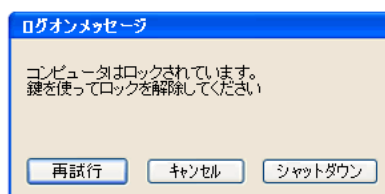
* Windows の設定によっては、「コンピュータのロック」画面は表示されない場合があります。

鍵を抜いた状態でログオンしようとすると、「コンピュータはロックされています。鍵を使ってロックを解除してください。」 と表示され、ログオンできません。

鍵を装着して「再試行」をクリックすると、「コンピュータのロックの解除」画面が表示され、パスワードを入力するとロックが解除され、ログオンすることができます。

●鍵を抜いた状態でパソコンを起動した場合

パソコンを起動すると「Windows へようこそ」画面が表示されます。

＊ Windows の設定によっては、「Windows へようこそ」画面は表示されずに「ログオンメッセージ」画面が表示されます。

鍵を抜いた状態でログオンしようとすると、「コンピュータはロックされています。鍵を使ってロックを解除してください。」と表示され、ログオンできません。

鍵を装着して「再試行」をクリックすると、「Windows へログオン」画面が表示され、パスワードを入力するとロックが解除され、ログオンすることができます。

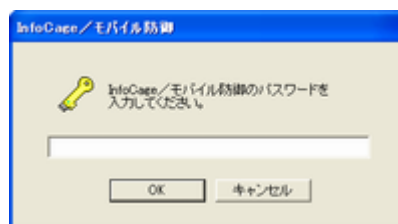
6.2　パスワード認証方式の場合

（画面イメージは Windows XP　Professional です）

再起動後に、通常のログオン画面が表示されます。
Ctrl＋Alt＋Del キーを押してください。

＊ Windows の設定によっては、「Windows　へようこそ」画面は表示されません。

ユーザパスワード入力画面が表示されます。
インストール時に設定したユーザパスワードを入力し、「OK」をクリックしてください。

＊ ユーザパスワードを 5 回連続で誤って入力すると、「OK」がクリックできなくなります。
その場合は「シャットダウン」をクリックして一旦シャットダウンした後、再度パソコンを起動してパスワード入力画面が有効になるまでしばらくお待ちください。
（すぐにパソコンを起動しても一定時間パスワードの入力はできません。）

「Windows へログオン」画面が表示され、ユーザ名と Windows ログオンパスワードを入力するとログオンすることができます。

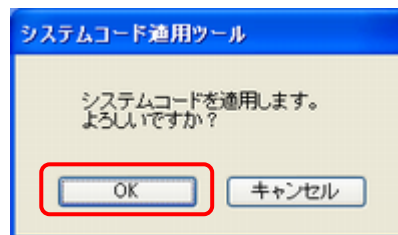
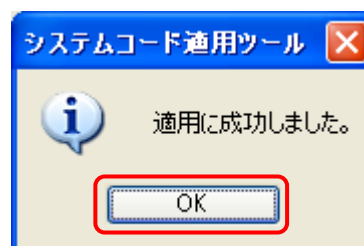
第7章　特定の FeliCa カードの設定

InfoCage モバイル防御をパスワード認証方式で運用しログオン認証に特定の FeliCa カードを使用するためには、システムコード (FeliCa カードに割り当てられている固有のコード) を適用する必要があります。インストール後にシステムコードを適用する場合は、システムコード適用ツールを使用します。
本設定は InfoCage モバイル防御の管理者の指示に従って操作してください。

* 本ツールは InfoCage モバイル防御 Ver3.5 以降がインストールされたパソコンで動作します。
* InfoCage モバイル防御の管理者によって FeliCa カードのシステムコードが設定されたセットアッププログラムでインストールした場合は、本設定は不要です。
* システムコード適用ツールは、コンピュータの管理者のユーザで実行してください。
* FeliCa カード認証は InfoCage モバイル防御をメディア鍵認証方式で運用している場合は使用できません。

Operation

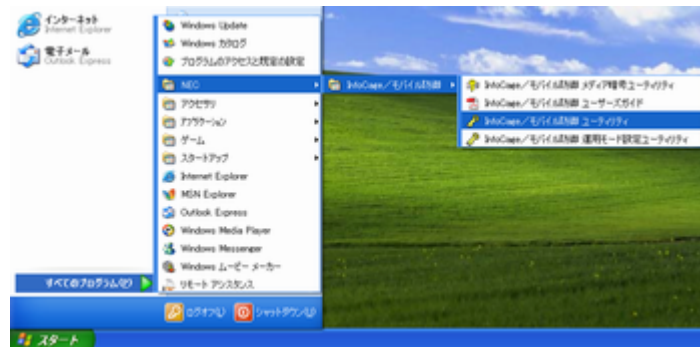
1. InfoCage モバイル防御の管理者から配布された mbscd.dat ファイルを、InfoCage モバイル防御をインストールしたフォルダ (通常は ¥Program Files¥NEC¥InfoCageCE) 内の¥Tools フォルダ内にある NmlStScd.exe と同じ場所に保存してください。

2. NmlStScd.exe を実行し、「OK」をクリックします。

3. システムコードが適用されました。「OK」をクリックしてください。

以上で終了です。
FeliCa カードの設定方法は、「InfoCage/モバイル防御 ユーザーズガイド」の「「認証設定」タブ」の項を参照してください。(パスワード認証方式のみ)

● InfoCage モバイル防御 ユーティリティを起動するには

スタートメニューから、［すべてのプログラム］－[NEC]－[InfoCage／モバイル防御]－[InfoCage／モバイル防御 ユーティリティ］をクリックしてください。

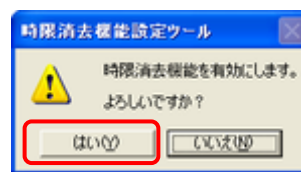
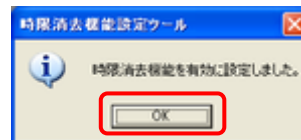
● InfoCage モバイル防御 ユーザーズガイドを参照するには

スタートメニューから、［すべてのプログラム］－[NEC]－[InfoCage／モバイル防御]－[InfoCage／モバイル防御 ユーザーズガイド］をクリックしてください。

第9章　時限消去機能について

時限消去機能を使用するためには「時限消去機能設定ツール」で有効にする必要があります。
以下の手順にて有効にしてください。

以下は、InfoCage モバイル防御がインストールされたパソコン上での操作手順です。

1. クライアント CD-ROM 内の¥2K_XP¥Tools¥時限消去機能設定ツール フォルダにある EnableTBM.exe を実行してください。

2. メッセージが表示されますので「はい」をクリックしてください。

3. 「OK」をクリックしてください。

以上で終了です。
時限消去機能の設定方法は、「InfoCage/モバイル防御 ユーザーズガイド」の「「時限消去設定」タブ」の項を参照してください。

第10章　セキュリティチップ(TPM)搭載のパソコンをお使いの場合

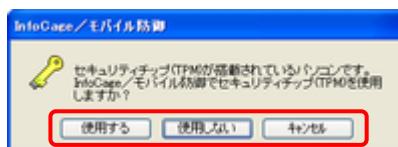
セキュリティチップ(TPM：Trusted Platform Module)とは、PC プラットフォームにおけるセキュリティ技術の業界団体 TCG (Trusted Computing Group)が策定した仕様に準拠した IC チップで、これを使用することにより、様々なセキュリティ機能を利用することが可能になります。

InfoCage モバイル防御のパスワード認証方式では、セキュリティチップ(TPM)の機能を使用することにより、さらに強固なセキュリティを実現できます。
セキュリティチップ(TPM)を使用する場合は、クライアント初期設定ツールにてカスタマイズされたセットアッププログラムを使ってインストールしてください。

セキュリティチップ(TPM)の使用について

セキュリティチップ(TPM)を有効に設定したセットッププログラムを使ってインストールした場合は、セキュリティチップ(TPM)を使用するかを選択することができます。
セキュリティチップ(TPM)を有効にするには、BIOS セットアップでセキュリティチップを「使用する」にし、セキュリティチップユーティリティをインストールしてください。

＊ セキュリティチップ(TPM)の設定方法についてはお使いのパソコンのマニュアルを参照してください。

InfoCage モバイル防御のパスワード認証方式をインストール後、InfoCage モバイル防御 ユーティリティの起動時に下記のメッセージが表示されます。
セキュリティチップ(TPM)を使用する場合は「使用する」を、使用しない場合は「使用しない」を、後で選択する場合は「キャンセル」をクリックしてください。
「キャンセル」をクリックした場合、TPM の使用を選択するまで InfoCage モバイル防御 ユーティリティの起動時にメッセージが表示されます。

注意事項

- セキュリティチップ(TPM)を使用するには、InfoCage モバイル防御のパスワード認証方式をインストールする前にセキュリティチップ用ドライバおよびユーティリティがインストールされている必要があります。
- BIOS のアップデートなどで設定値を初期化した場合、アップデート後にセキュリティチップの値を必ず元に戻してください。
- セキュリティチップ(TPM)を使用している場合、セキュリティチップユーティリティをアンインストールしないでください。アンインストールすると暗号化されたファイルにアクセスできなくなります。
- セキュリティチップ(TPM)を使用している場合、BIOS でセキュリティチップを「使用しない」に設定を変更したり、設定値の初期化をしたりすることは絶対にしないでください。これらの操作を実行した場合、暗号化されたファイルにアクセスできなくなります。

第11章 トラブルシューティング

インストール時に 「1607：InstallShield Scripting Runtime をインストールできません。」というメッセージが表示され、インストールできない。

このエラーは、InstallShield が次のような原因で正常に動作していないときに表示されます。

(1) 管理者権限の無いユーザでログオンしている。
- インストールする際のユーザ権限は、コンピュータの管理者（アドミニストレータ権限）で行ってください。

(2) IDriver.exe が正しく登録されていない。
- Windows のコマンドプロンプトから以下のコマンドを実行して、IDriver.exe を登録しなおしてください。

¥Program Files¥CommonFiles¥InstallShield¥Driver¥7¥Intel32¥IDriver.exe/REGSERVER （注1）

※ Windows が C ドライブにインストールされている場合の例です。それ以外のドライブにインストールされている場合には、該当するドライブ文字に置き換えてください。
※ （注1）下線部はお使いの環境によって異なる場合があります。

(3) 同時に複数のインストーラが起動している。
- 誤って Setup.exe を複数実行してしまった場合、一旦全てのインストーラを終了してから、再度インストールを行ってください。

(4) Windows インストーラ(msiexec.exe)が正しく登録されていない。
- 任意の場所（デスクトップ等）に「新規作成」でテキストファイルを作成し、ファイルの拡張子を.txt から.msi に変更してください。
アイコンがインストーラのアイコンに変わるか確認します。
アイコンがインストーラのアイコンに変わらない場合は、コマンドプロンプトで以下のコマンドを実行してください。
C:¥Windows¥System32¥msiexec.exe /REGSERVER

※ Windows XP が C ドライブにインストールされている場合の例です。
それ以外のドライブにインストールされている場合には、該当するドライブ文字に置き換えてください。
また、OS が異なる場合はシステムフォルダ名を置き換えてください。

(5) Windows XP で、「SUBST」コマンドで作成した仮想ドライブからインストールを実行している。
- SUBST コマンドによる仮想ドライブを解除してください。

* その他については「InfoCage/モバイル防御 ユーザーズガイド」のトラブルシューティングをご参照ください。

● **商標について**

- Microsoft および Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- VMware は米国 VMware, Inc.の商標です。
- StandbyDisk、StandbyDisk Solo、および StandbyDisk Solo RB は、StandbySoft LLC／(株)ネットジャパンの商標です。
- FINALDATA は、FINALDATA INC.または AOS テクノロジーズ株式会社の登録商標です。
- V2i Protector は PowerQuest Corporation の商標です。
- DirectCD および Easy CD Creator は、Adaptec 社の商標です。
- B's CliP および B'sRecorder Gold は、株式会社ビー･エイチ･エーの登録商標です。
- Rapid Restore および Rescue and Recovery は IBM Corporation の商標です。
- eTrust は Computer Associates International Inc.の登録商標です。
- Norton AntiVirus、Symantec AntiVirus、Norton Utilities および Norton SystemWorks は Symantec Corporation の米国およびその他の国における登録商標または商標です。
- NetWizard は Attachmate Corporation の商標です。
- RecordNow! は Sonic Solutions 社の登録商標です。
- FeliCa は、ソニー株式会社の登録商標です。
- Swipe はティアック株式会社の商標です。
- BIGLOBE は日本電気株式会社の商標です。
- InfoCage は日本電気株式会社の登録商標です。
- その他、本マニュアルに記載されている会社名、商品名は各社の商標または登録商標です。
- このマニュアルの一部、又は全部を流用･複写することはできません。

本マニュアル中のサンプル画面で使用している名称は、全て架空のものです。実在する品名、団体名、個人名とは一切関係ありません。

● **免責事項**

本書及び本システムは、ライセンス契約に基づいて使用することができます。ライセンス契約で明示的に定められていないかぎり、日本電気株式会社は製品、及びその関連文書について、明示的にも暗黙的にも、商品性に関する保証、特定目的への適合性に関する保証、取り扱い、使用、または取引行為に伴う保証について一切の責任を負いません。

InfoCage モバイル防御 Ver 3.6
インストールガイド

日本電気株式会社
東京都港区芝５丁目７番１号
TEL(03)3454-1111（大代表）

MI360-0707-X01